Accommodation Addresses for Secure Community Networks

4G−3

Yoshiyuki HAMAOKA, Kazuhiko NAGATA, Takemi NISASE and Hiroyuki ICHIKAWA

NTT Information Sharing Platform Laboratories, NTT Corporation

I. INTRODUCTION

Background. Community networks are groups of users who have a specific common purpose on the Internet. Internet Service Providers (ISPs) face challenges in terms of making the users' experience of such networks, more secure and enjoyable. One aspect of this is protecting their personal information of users, and, in particular, the fixed IP address of users, which are becoming more important as a way of identifying him/her. Discussion of the need for anonymity at the IP layer has commenced [1]. Some existing network address translation (NAT) [2], [3] and proxy server [4], [5] techniques allow the relaying of communications in which the IP addresses of users are concealed, but there are limits on scalability, compatibility with applications and so on.

Our contribution. Firstly, we present the concept of *Accommodation Address (AA) service*, our term for a service from an ISP in which communications are relayed with the fixed IP addresses of users concealed. The term was derived from the postal accommodation address service. Secondly, we propose the use of a privacy gateway (PGW) as a way of overcoming the problems of existing NAT and proxy server techniques.

II. ACCOMMODATION ADDRESS SERVICE

Overview. In the typical community network, users have little trust in the parties with whom they communicate. A reliable intermediary can thus help the user by concealing the user's personal information. This is one role of the ISP. With the growing number of continuous connection services and IPv6 users, the fixed IP address of a user is coming to be among the most important items of personal information. The accommodation address service is shown in figure 1. The ISP makes it possible for User A to use accommodation address x in community X and accommodation address y in community Y, while concealing the fixed address of User A.

Yoshiyuki HAMAOKA is with NTT Information Sharing Platform Laboratories, NTT Corporation, 3-9-11, Midori-cho, Musashino-shi, 180-8585, Japan. E-mail: hamaoka.yoshiyuki@lab.ntt.co.jp

Service Scenario. When a user decides that the user wants to use an AA in a community before entering communications with that community, the user asks the ISP to add an entry to the user's fixed IP address at a AA and informs the user of the assigned AA. The user then discloses the assigned AA to the community instead of the user's fixed IP address.

Requirements. The basic requirements for accommodation address service are that i) the user must be able to use different accommodation addresses in different communities so that the user is able to establish different identities in different communities, and to choose whether or not to use the accommodation address service, ii) the system must work with all IP applications, iii) it must be scalable from the ISP's point of view and iv) it must have a high level of performance for QoS-critical applications.

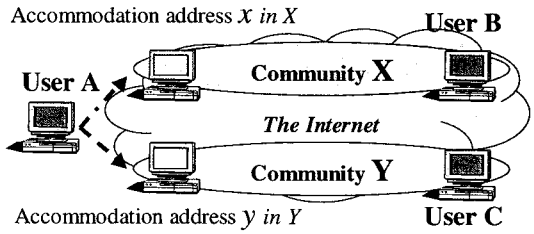

Figure 1. Accommodation address service.

III. NAT AND PROXY SERVER

NAT. NAT is mainly used to translate addresses from isolated private addressing domains to external global addressing domains. NAT is located in the IP routing path between User A and User B. But it is transparent from their point of view. The NAT intercepts packets from User A, translates the source address (SA) from the address of User A to a NAT address without modifying the datagram, and sends the translated packets on to ward User B.

Proxy server. A proxy server is mainly used to cache HTTP content [6]. The proxy server receives packets from User A, examines the contents of the packets at the application layer, determines the destination for the message, then sends the message onwards to User B.

IV. PRIVACY GATEWAY

Overview. We propose a new technique of using a PGW that has a variety of addresses in its network interfaces; these include the accommodation address (AA) that is related to the address of the user and the proxy address (PA) that is related to the address of the user's communication partner. It has a special NAT function that translates both SA and DA. A user is able to conceal the user's fixed IP address by receiving packets at the user's AA and sending packets to the PA of the communication partner.

The procedure using a PGW in communication is shown in figure 2. In the forward direction, PGW translates both the SA, from the address of User A to the AA of User A, and the DA, from the PA to the address of User B. In the opposite direction, it translates the SA, from the address of User B to the PA of User B, and the DA, from the AA of User A to the address of User A.

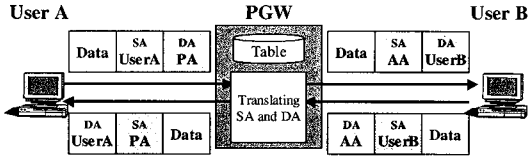

Figure 2. Overview of PGW.

Algorithm inside PGW. The algorithm used inside the PGW is shown in figure 3. Firstly, the PGW inspects the DA of the received packet and searches the network address translation table to determine whether it is in the forward or backward direction and which user is intended to receive it. Secondly, it inspects the SA and searches it to determine which address is related to the sending user. Thirdly, it translates both the SA and the DA according to the entries found in the table.

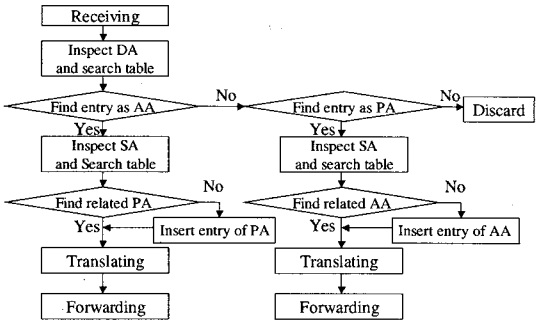

Figure 3. Algorithm inside PGW.

Implementation. For practical use, the PGW may include an application-level gateway (ALG) function for those applications that use IP addresses inside the datagram of IP packets.

V. DISCUSSION

We discuss the advantages of our PGW by comparing it with the existing NAT and proxy server approaches, in term of the four requirements above in section II.

Control. The PGW technique allows a user to change his/her accommodation address according to the community within which he/she is communicating, and to choose whether or not to use the accommodation address service by changing the DA of a set of sent packets. NAT techniques do not provide such facilities.

Scalability. The PGW technique achieves a high degree of scalability by processing only those packets for the accommodation address service, because a user is able to choose whether or not to have the PGW process sent packets. NAT technique is only suitable for small groups of users, because it processes all packets even though most of them are not for the address translation service.

Compatibility with Applications. The PGW technique is applicable to all IP applications that do not need an ALG, because it works at the network layer. The proxy server is able to support only certain applications, because it works at the application layer.

Performance. The lower complexity of processing in the PGW technique gives it better performance than a proxy server. PGW only translates packet headers and does not reassemble packets, while, on the other hand, proxy servers terminate the connection at the application-layer level and reassemble packets.

VI. CONCLUSION AND FUTURE WORK

Our new technique of using a PGW effectively provides an accommodation address service that overcomes the problems of existing techniques.

We plan to extend the essential concept of the accommodation address service and PGW technique by adding new functions for improving community networks and firewall, user-authentication function and AA persistence functions, etc.

REFERENCES

[1] S. Bradner, "The Nymip Effort", http://nymip.velvet.com/
[2] Bill Dutcher, "The NAT Handbook," ISBN0-471-39089-5.
[3] K. Egevang and P. Francis, "The IP Network Address Translator," Internet Request for Comments (RFC1631), May 1994.
[4] R. Fielding et al, "Hypertext Transfer Protocol -- HTTP/1.1," Internet Request for Comments (RFC2068), January 1997.
[5] "Squid Web Proxy Cache," http://www.squid-cache.org/.